REMARKS

The Office Action dated November 18, 2004 has been received and reviewed by the applicant. Claims 1-16 are in the application. Claims 1-16 stand rejected. Claims 1 and 9 are amended.

The drawings are objected to because they are handwritten and the text is unclear. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office Action. In response, drawings are submitted herewith under separate cover.

Claims 1-16 are rejected under 35 USC 102(e) as being anticipated by Carr et al. (US 6,788,800). First, it is instructive to point out the meaning of term used in the '800 Patent. It is noted that the term watermark is defined in column 1, line 22-27:

> Research in the field of steganography (also called "data hiding") offers promising technology for combating counterfeiting and piracy. One form of steganography is referred to in popular literature as digital watermarking. **Digital watermarking is a process for modifying a host signal or object to embed a machine-readable code into the host**. The host may be modified such that the embedded code is imperceptible or nearly imperceptible to the ordinary observer upon viewing or playback, yet may be detected through an automated detection process.

In summary, watermarking is "***additional***" data is embedded into a host signal which can be subsequently deciphered. This is entirely different from "encrypting" as in the claimed invention where no additional data is added and the signal is scrambled. Encryption means "putting data into a secret code so it is unreadable except by authorized users" and "the scrambling of data to prevent anyone other than the intended recipient from reading the information." (see the attached definition from techdictionary.com).

Turning now to the rejection, the rejection cites column 7, lines 49-58 as disclosing element (a) of claim 1, "converting a captured image into a 3-D wire mesh representing the three-dimensional exterior of the image having a plurality of line segments...". It is respectfully submitted that column 7, lines 49-58 discloses moving the additional data (watermark) into various locations of a

signal. It does not disclose "converting an image into a 3-D wire mesh." It does not mention a 3-D wire mesh and is entirely restricted to a 2-dimensional signal, such as electronic representations of documents and the like. Wire mesh is defined on page 3, lines 16-18 of the present invention as "a plurality of interconnecting segments 35 that forms a model of the exterior shape of the input image." It is respectfully submitted that US Patent '800 does not teach or suggest a wire mesh.

The rejection cites column 5, lines 27-46 as disclosing element (b) of the claimed invention of "providing movement data, which directs movement of the wire mesh data." It is courteously submitted that, since a wire mesh is not disclosed, clearly there is not movement data associated with it. The cited section of the '800 Patent teaches that the object in which the additional data (watermark) is embedded may be software, music or the like and that these objects (software, music and the like) may be stored on some sort of media. Clearly, this is not movement data for a wire mesh.

The rejection cites column 6, lines 32-50 as disclosing element (c) of "electronically transmitting the wire mesh...". Since there is no wire mesh, obviously there is no transmission.

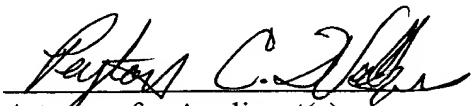
The rejection cites column 4, lines 1-29 as disclosing element (d) "encrypting the movement data...". This section discloses that, once additional data is added, the additional data is then encrypted. In the claimed invention, there is no watermark (additional data) that is encrypted. Movement data is the entire signal or data and no watermark is added. Secondly, the encryption in the '800 Patent is not "movement data" but is instead a watermark.

Consequently, it is courteously submitted that the claimed invention is not taught or suggested by the '800 Patent. Claim 9 includes substantially the same limitations as claim 1 and is patentable for the same reasons as claim 1.

Should the Examiner consider that additional amendments are necessary to place the application in condition for allowance, the favor is requested of a telephone call to the undersigned counsel for the purpose of discussing such amendments.

For the reasons set forth above, it is believed that the application is in condition for allowance. Accordingly, reconsideration and favorable action are respectfully solicited.

Respectfully submitted,



Attorney for Applicant(s)
Registration No. 36,390

Peyton C. Watkins/lam
Rochester, NY 14650
Telephone: 585-477-8282
Facsimile: 585-477-4646

If the Examiner is unable to reach the Applicant(s) Attorney at the telephone number provided, the Examiner is requested to communicate with Eastman Kodak Company Patent Operations at (585) 477-4656.

Amendments to the Drawings:

Formal drawings are submitted herewith under Separate Letter to the Draftsperson. For the convenience of the Examiner, a copy of the formal drawings are also attached with this amendment.

techdictionary.com

Home
Search
Search Tips
Domain List
Chat/SMS Terms
Emoticons
File Extensions
Suggest Term
Bookmark Us
Add To Your Site
Tell A Friend
TechTips & Links
Tech News
Virus News
Advertise
About/Site Map

Search Results

Term:	Definition:
conventional encryption	A form of encryption in which sender and receiver share with each other a secret key to decrypt messages sent between them. Conventional encryption, also called private key encryption, is different from public key encryption in which both sender and receiver have the public key, but each has a private key which is not shared.
public-key encryption	A way of encrypting messages in which each user has a public key and a private key. Messages are sent encrypted with the receiver's public key; the receiver decrypts them using the private key. Using this method, the private key never has to be revealed to anyone other than the user.
private key encryption	A form of cryptography in which sender and receiver have the same key or similar keys.
secret key encryption	A form of cryptography in which sender and receiver share a secret key.
symmetric encryption	A form of cryptography in which sender and receiver have the same key.
Encryption	Putting data into a secret code so it is unreadable except by authorized users. The "scrambling" of data to prevent anyone other than the intended recipient from reading the information. Encryption protects data during actual transmission across the public network.
encoding remediation technique (encryption, offset counter format, integer date format)	Unlike field expansion, encoding allows current field sizes to be maintained by storing additional information into existing fields. A more efficient use of bits may allow inclusion of century information. (There is a general agreement within the industry that there is no single method of remediation that can be applied to all situations.)
Data Encryption Standard	(DES) An unclassified crypto algorithm adopted by the National Bureau of Standards for public use. A cryptographic algorithm for the protection of unclassified data, published in Federal Information Processing Standard (FIPS) 46. The DES, which was approved by the National Institute of Standards and Technology (NIST), is intended for public and government use.

SEARCH-AGAIN